REMARKS

Claims 1, 13, 14 and 26-30 have been amended.

The Examiner has rejected applicant's claims 1, 3-6, 8-14, 16, 19 and 21-30 under 35 USC 103(a) as being unpatentable over the Wright, et al. (U.S. Publication No. 2002/0016910) patent application in view of the Saliba, et al. (U.S. Publication No. 2001/0037315) patent application publication in further view of the Anderson (U.S. Publication No. 2002/0052923) patent application publication. Applicant has amended applicant's independent claims 1, 13, 14 and 26-30 and with respect to these claims, as amended, and their respective dependent claims, the Examiner's rejections are respectfully traversed.

Applicant has amended applicant's independent claims 1, 13, 14 and 26-30 to better define applicant's invention. In particular, applicant's independent claims 1 has been amended to recite a communication system having a server for providing a Web E-mail service to a Web browser of a client, wherein said server comprises: management means for managing a secret key for decrypting an encrypted E-mail message addressed to a user's mail address, the E-mail message being encrypted by a public key corresponding to the user's mail address, wherein the secret key corresponding to the user's mail address for decrypting the encrypted E-mail message is not managed by the Web browser of the client; web encryption communication means for establishing a Web encryption communication with the Web browser of the client, and communicating with the Web browser of the client by the Web encryption communication established by said web encryption communication means; authentication means for executing authentication of a use allowance of the secret key managed by said management means to the Web browser of the client when the Web browser of the client requests to decrypt the

encrypted E-mail message while the server communicates with the client by said established Web encryption communication; decrypting means for making a decrypted E-mail message by decrypting the encrypted E-mail message using the secret key managed by said management means, the secret key corresponding to the user's mail address, in the case where the use allowance of the secret key managed by said management means is authenticated by said authentication means; and transmission control means for controlling to transmit the decrypted E-mail message decrypted by said decrypting means to the client through the Web encryption communication established by said web encryption communication means, the decrypted E-mail message being not re-encrypted by a public key when the decrypted E-mail message is transmitted by said transmission control means. Applicant's independent claims 13, 14 and 26-30 have been similarly amended.

Applicant's invention of the above claims is a characterized by controlling to transmit a decrypted E-mail message decrypted by a decrypting means to a client through a Web encryption communication established by a web encryption communication means. More particularly, the invention of these claims is further characterized in that the decrypted E-mail message is not re-encrypted by a public key when the decrypted E-mail message is transmitted.

In contrast, in the Wright, et al. patent application, a file is uploaded in a condition of an encrypted file 32 when a file is uploaded from a client computer to a server. Also, in this application, a file is downloaded in a condition of an encrypted file 32 when a file is downloaded from a server to a client computer. That is, in Write, et al. patent application, in the transmission between a server and a client, a file is transmitted as an encrypted file. The encrypted file 32 is decrypted in the client. (paragraph [0063] and [0064]).

More specifically, paragraphs [0063] and [0064] of Write, et al publication, disclose

that an encrypted document 32 is encrypted from a file 30 with a public key 8 in a web browser 5 of the client. Then, the generated encrypted file 32 is uploaded onto the data server and stored into the data storage unit 12. Next, when a user requests to download a file, the encrypted document 32 and the Encrypted Private Key 9 are downloaded to the user's local machine. The user then inputs the user's key phrase 43 into the User Application 19 and the Encrypted Private Key 9 downloaded to the user's local machine is decrypted to generate the Clear text Private Key 10. The Clear text Private Key 10 and the Retrieved Encrypted Document are finally passed through the Public Key Crypto Engine 7 to produce the Decrypted Document 39.

Therefore, as stated above, in the in Write, et al. patent application, in the transmission between a server and a client, a file is transmitted as an encrypted file. The patent application thus fails to teach or suggest the feature of the present invention characterized in that the decrypted E-mail message is not re-encrypted by a public key when the decrypted E-mail message is transmitted.

The Anderson patent application has similar failings. This application discloses that a server decrypts an encrypted message with the secret key of the server. Afterward, the server encrypts the decrypted message with the public key of a client and transmits the encrypted message. In the client, the encrypted message is decrypted with the secret key managed by the client. That is, in the transmission between a server and a client, a file is transmitted as an encrypted file.

More particularly, paragraph [0036] of the Anderson patent application discloses that when a message is transmitted as an encrypted file, Message Sender encrypts with the obtained public key of the server the message and the encrypted message is transmitted to the MDS system for further distribution (at steps 320 and 330). The Anderson patent also discloses

in FIG. 5 that when Message Distributor receives an encrypted message, the encrypted file is decrypted with a secret key of the server to create an entry in the Message Tracking Table for the message. Specifically, a subroutine at step 510 determines if the received message is encrypted, and if so continues at step 515 to decrypt the message with the server's private key. After step 515, or if it was determined in step 510 that the received message was not encrypted, the subroutine continues at step 520 to create an entry in the Message Tracking Table for the message. If it is determined in step 540 that the received message was encrypted, the public key for each recipient is retrieved to encrypt a copy of the message indicator with the retrieved key and send the encrypted message indicators to the appropriate recipients at step 545. And then, as described in lines 5 to 9 of the paragraph [0044] of the Anderson patent application, the recipient computer decrypts the received message with the secret key of the recipient computer.

Thus, in the Anderson patent application, as above-stated, in the transmission between a server and a client, a file is transmitted as an encrypted file. Therefore, this patent application also fails to teach or suggest the feature of the present invention characterized in that the decrypted E-mail message is not re-encrypted by a public key when the decrypted E-mail message is transmitted.

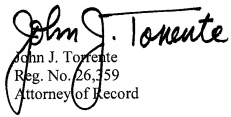
The Saliba, et al. patent application merely discloses the use of SSL transmission. Hence, this patent application also fails to teach or suggest the feature of the present invention characterized in that the decrypted E-mail message is not re-encrypted by a public key when the decrypted E-mail message is transmitted.

As a result, the Wright, et al., Anderson and Saliba, et al. patent applications fail to teach or suggest the invention of applicant's amended independent claims 1, 13, 14 and 26-30, and their respective dependent claims.

In view of the above, it is submitted that applicant's claims, as amended, patentably distinguish over the cited art of record. Accordingly, reconsideration of these claims is respectfully requested.

Dated: May 30, 2007

Respectfully submitted,



John J. Torrente
Reg. No. 26,559
Attorney of Record

COWAN, LIEBOWITZ & LATMAN, P. C.
1133 Avenue of the Americas
New York, New York 10036
T (212) 790-9200